Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Авдадаев Джамал Геланиевич

Содержание

Список иллюстраций

Список таблиц

1 Введение

1.1 Цель работы

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

2 Процесс работы

2.1 Создание пользовательской службы firewalld

2.1.1 Копирование и подготовка файла службы

На сервере был создан файл пользовательской службы на основе стандартного описания SSH.
После копирования и перехода в каталог `/etc/firewalld/services/` было просмотрено содержимое файла `ssh-custom.xml`.

```
[root@server.dgavdadaev.net server]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.dgavdadaev.net server]# cd /etc/firewalld/services/
[root@server.dgavdadaev.net services]# cat ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted
communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the open
ssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.dgavdadaev.net services]#
```

Рис. 2.1: Просмотр оригинального файла ssh-custom.xml

Структура файла представляет собой XML-документ:

- Заголовок XML включает версию и кодировку.
- Корневой элемент `<service>` объединяет параметры одной службы.
- Элемент `<short>` содержит краткое имя сервиса.
- Элемент `<description>` описывает назначение службы.
- В блоке `<port>` указан протокол и номер порта, который следует открыть.

2.1.2 Модификация службы

Файл описания был открыт в редакторе.

В него внесены изменения:

- порт изменён на 2022;
- описание дополнено, чтобы указать, что файл является модифицированным.

Рис. 2.2: Редактирование ssh-custom.xml

2.1.3 Проверка списка служб FirewallD

Выведен список всех доступных служб.

Пользовательская служба ещё не отображается в перечне.

После перезагрузки конфигурации отображены обновлённые списки доступных и активных служб.

Новая служба стала видимой, но пока не активной.

```
[root@server.dgavdadaev.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audit a
usweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testn
et-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd condor-collector
 cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm
dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-
replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap ima
ps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshe
ll kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls ligh
tning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqt
t mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut o
pentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privox
y prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sent
inel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp
 smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom statsrv steam-lan
-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-re
lay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vd
sm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-disco
very-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server za
bbix-trapper zabbix-web-service zero-k zerotier
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.dgavdadaev.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.dgavdadaev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.dgavdadaev.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.dgavdadaev.net services]# firewall-cmd --reload
success
[root@server.dgavdadaev.net services]#
```

Рис. 2.3: Перезагрузка и проверка

2.1.4 Активация пользовательской службы

Служба была добавлена в набор активных.

После этого она стала отображаться среди включённых.

Затем служба была добавлена в постоянную конфигурацию и правила firewall были перезагружены.

2.2 Настройка перенаправления порта

На сервере настроено перенаправление трафика с порта 2022 на стандартный порт SSH — 22.

```
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.dgavdadaev.net services]#
```

Рис. 2.4: Настройка forward-port

2.2.1 Проверка работы с клиента

С клиентской машины выполнено подключение к серверу по SSH через порт 2022.

Соединение успешно установлено, что подтверждает корректность перенаправления.

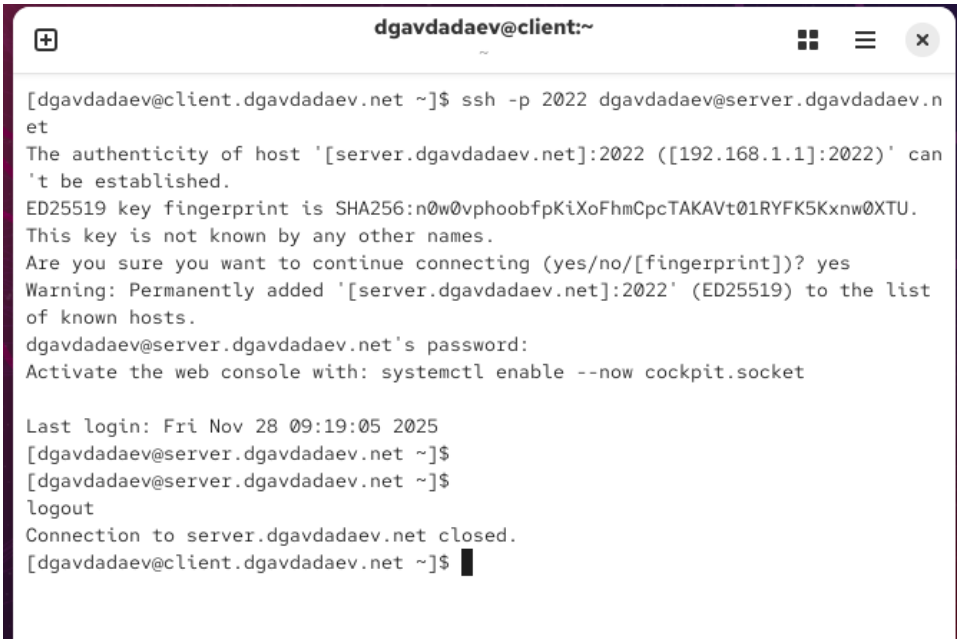

Рис. 2.5: Подключение к серверу через порт 2022

2.3 Включение IPv4 forwarding и маскарадинга

Проверено состояние параметра пересылки пакетов.

Далее был включён IPv4 forwarding и создан конфигурационный файл, содержащий этот параметр.

После применения настроек активирован маскарадинг и перезагружена конфигурация firewall.

```
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.dgavdadaev.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.dgavdadaev.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.dgavdadaev.net services]# firewall-cmd --reload
success
[root@server.dgavdadaev.net services]#
```

Рис. 2.6: Настройка forwarding и masquerading

2.4 Подготовка конфигурации для Vagrant

В каталоге `/vagrant/provision/server/` создана структура директорий для хранения конфигураций FirewallD и системных параметров:

- директория для служб FirewallD;
- директория для файлов sysctl.

В эти каталоги были помещены:

- файл службы `ssh-custom.xml`;
- файл `90-forward.conf`.

Также был создан файл `firewall.sh`.

```
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# cd /vagrant/provision/server/
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.dgavdadaev.net server]# cp -R /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/servic
es
[root@server.dgavdadaev.net server]# cp -R /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.dgavdadaev.net server]# touch firewall.sh
[root@server.dgavdadaev.net server]#
```

Рис. 2.7: Подготовка структуры каталогов

2.4.1 Содержимое файла firewall.sh

Скрипт включает операции копирования конфигураций, регистрации службы, настройки перенаправления порта, включения masquerading и восстановления контекстов SELinux.

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc
echo "Configure masquerading"
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc
```

Рис. 2.8: Содержимое firewall.sh

3 Итоги

3.1 Вывод

В процессе выполнения работы была создана пользовательская служба firewalld, настроено перенаправление порта, включено пересылание IPv4-пакетов и маскарадинг. Проверена работа SSH-доступа через новый порт. Конфигурационные файлы были вынесены в директорию Vagrant provisioning, а для автоматизации создан скрипт firewall.sh. Полученная конфигурация успешно функционирует и может применяться при повторном развёртывании виртуальной машины.

3.2 Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

В каталоге `/etc/firewalld/`, включая подкаталоги `services/`, `zones/` и другие, где пользователь может размещать собственные конфигурации.

2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?

Строку с определением порта в XML-формате:

```
<port protocol="tcp" port="2022"/>
```

3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?

Команда для вывода списка всех доступных служб:

```
firewall-cmd --get-services
```

4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?

NAT — общий механизм преобразования адресов и портов при прохождении пакетов между сетями.

Маскарадинг — разновидность NAT, при которой внешний IP выбирается автоматически, обычно используется при динамическом IP-адресе интерфейса.

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?

Команда перенаправления входящего трафика:

```
firewall-cmd --add-forward-port=port=4404:proto=tcp:toaddr=10.0.0.10:toport=22
```

6. Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?

Команда активации маскарадинга:

```
firewall-cmd --zone=public --add-masquerade --permanent
```